REMARKS

Favorable reconsideration of this application as presently amended and in light of the following discussion is respectfully requested.

Claims 1-10, 12-26, 28-41, 43, and 44-47 are pending in the present application. The present amendment amends Claims 1, 5, 16, 20, 32 and 36 and adds new Claims 45-47, all without the introduction of any new matter.

In the outstanding Office Action, Claims 1-4, 16-19 and 32-35 were rejected under 35 U.S.C. 102(e) as anticipated by Riggins (U.S. Patent No. 6,766,454). Claims 5-13, 20-23, 25-27, and 36-43 were rejected under 35 U.S.C. 103(a) as unpatentable over Riggins in view of Hudson et al. (U.S. Patent No. 6,055,637, herein "Hudson"). Claims 14 and 44 were rejected under 35 U.S.C. 103(a) as unpatentable over Riggins in view of Hudson further in view of Scheifler et al. (U.S. Patent No. 6,138,238, herein "Scheifler"). Claim 15 was rejected under 35 U.S.C. 103(a) as unpatentable over Riggins in view of Hudson further in view of Montulli (U.S. Patent No. 5,774,670). Claims 24, 28-29 were rejected under 35 U.S.C. 103(a) as unpatentable over Riggins in view of Hudson further in view of Daly et al. (U.S. Patent No. 5,875,394, herein "Daly"). Claim 30 was rejected under 35 U.S.C. 103(a) as unpatentable over Riggins, Hudson, and Daly and further in view of Susaki et al. (U.S. Patent No. 6,189,032, herein "Susaki"). Claim 31 was rejected under 35 U.S.C. 103(a) as unpatentable over Riggins, Hudson, and Daly in view of Montulli.

To vary the scope of protection in the claims, new dependent Claims 45-47 are presented for examination. New Claims 45, 46 and 47 depend upon independent Claims 1, 16 and 32, respectively, and recite "said electronic badge includes a period of time during which the electronic badge is valid." This feature finds non-limiting support in Applicant's specification as originally filed, for example from page 11, line 27, to page 12, line 3. Therefore the new claims are not believed to raise a question of new matter.

To clarify Applicant's invention, independent Claims 1, 16 and 32 are amended. In particular, independent Claim 1 is amended to recite "a password protection unit adapted to authorize transmission of said electronic badge to the visitor's computer based on authentication of a password, and adapted to embed the password into the electronic badge." Independent Claim 16 (method claim) and Claim 32 (device claim) are amended to recite an analogous feature. This feature finds non-limiting support in Applicant's specification as originally filed, for example at page 9, lines 18-21.

To clarify Applicant's dependent claims, dependent Claims 5, 20 and 36 are amended to further recite that the applet includes the password in encrypted form. This feature finds non-limiting support in Applicant's specification at page 2, lines 2-3.

In light of the amendments to independent Claims 1, 16 and 32, Applicant respectfully traverses the rejection of Claims 1-4, 16-19, and 32-53 under 35 U.S.C. 102(e), and requests reconsideration of the rejection, as next discussed.

Briefly recapitualting, Applicant's Claim 1 relates to a telecommunications system configured to provide a visitor's computer with access to applications. The system includes: an application computer storing the at least one application; a firewall protecting the application computer; an administration computer operatively linked to the application computer, configured to generate an electronic badge, and configured to transmit the electronic badge to the visitor's computer, the electronic badge including access rights conferring access of the visitor's computer through the firewall to the applications; and a password protection unit adapted *to authorize transmission of the electronic badge to the visitor's computer based on authentication of a password*, and *configured to embed the password into the electronic badge*.

As explained in Applicant's specification at page 2, lines 11-13, Applicant's Claim 1 improves upon background telecommunication systems configured to provide a visitor's

computer with access to at least one application, since the invention facilitates the secure

control of access to a secure computer facility via exchange of identity badges over the

internet.

Turning now to the applied references, <u>Riggins</u> describes a system for using an

authentication applet to identify and authenticate a user in a computer network.[1] <u>Riggins</u>

thereby presents a solution that "never send[s] the password itself across the computer

network and thus never compromise the password by transmission across unsecured

channels."[2] <u>Riggins,</u> however, fails to teach or suggest

> a password protection unit adapted *to authorize transmission of
> said electronic badge* to the visitor's computer based on authentication of
> a password, and adapted to *embed the password into the electronic badge.*

as recited in Applicant's amended, independent Claim 1. First, <u>Riggins</u> fails to teach or

suggest that the password protection unit is adapted *to authorize transmission of said*

electronic badge to the visitor's computer based on authentication of a password. In <u>Riggins,</u>

the password module 1155 is embedded into <u>Riggins'</u> authentication applet 955,[3] therefore,

the authentication applet has first to be executed, and then a password is authenticated. In

particular, <u>Riggins</u> explicitly teaches that the authentication applet 955 is first downloaded to

servlet host engine 386, in a step 530.[4] Thereafter, the <u>Riggins'</u> applet 955 is executed (step

535), and access to the service requested by the user is provided in a *later step 540.* The

details of different embodiments of <u>Riggins'</u> step 540 are shown in Figures 8A-8C, wherein

the downloaded applet 288 is accessing a keysafe 395 for authentication.[5] Accordingly,

downloading an applet, executing it, and thereafter authenticating passwords, as taught by

<u>Riggins,</u> *is not* a password protection unit adapted *to authorize transmission of said*

---

[1] See <u>Riggins</u> in the Abstract.
[2] See <u>Riggins</u> at column 2, lines 63-66.
[3] See <u>Riggins</u> at column 12, lines 52-60, and in corresponding Figure 11B.
[4] See <u>Riggins</u> at column 8, lines 1-4, and in corresponding Figure 5.
[5] See <u>Riggins</u> for example at column 9, lines 5-20.

14

electronic badge to the visitor's computer based on authentication of a password, as recited in Applicant's amended, independent Claim 1.

In addition, Riggins fails to teach or suggest that the password protection unit is also adapted to *embed the password into the electronic badge*. Riggins clearly explains that passwords are not sent over the network,[6] and that the downloaded applet 288 accesses a keysafe 395. Riggins' keysafe 395 is stored in the data storage device 360 of the global server 106,[7] and is accessed by the downloaded applet 288 after its execution for authentication of services and user (step 540).[8] Riggins also recites that "[t]he applet 955, in coordination with user input, computes and forwards a proper response to the challenge 965 back to the global server 920. The global server 920 verifies the response."[9]

Therefore, a downloaded applet 288 accessing a datasafe 395 including passwords for authentication, as taught by Riggins, *is not* a password protection unit is adapted to embed the password into the electronic badge, as recited in Claim 1. Applicant also respectfully submits that the Claim 1 password for authentication and embedded into the electronic badge is *the same password*.

Therefore, the applied reference fails to teach or suggest every feature recited in Applicant's claims, so that Claims 1-4, 16-19 and 32-35 are patentably distinct over Riggins. Accordingly, Applicant respectfully traverses, and requests reconsideration of, the rejection based on Riggins.[10]

Further Applicant respectfully submits that the dependent claims are also believed to be patentably distinct over the applied references, as next discussed.

---

[6] See Riggins at column 2, lines 63-66.
[7] See Riggins for example from column 6, line 66, to column 7, line 7, and in corresponding Figure 3.
[8] See Riggins at column 9, lines 5-67, Figures 8A-8C.
[9] See Riggins at column 11, lines 2-12.
[10] See MPEP 2131: "A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference," (Citations omitted) (emphasis added). See also MPEP 2143.03: "All words in a claim must be considered in judging the patentability of that claim against the prior art."

Regarding the rejection of Applicant's dependent Claims 8, 23 and 39 under 35

U.S.C. §103(a), Applicant respectfully traverses the rejection, and requests reconsideration of

the rejection, as next discussed.

Applicant's Claim 8 recites "said administration computer is configured to be linked

to a web server that issues said electronic badge to the visitor's computer *in response to said*

authorization" (emphasis added). However, the applied references, <u>Riggins</u> and/or <u>Hudson</u>,

taken individually or in any proper combination, fail to teach or suggest such a feature.

<u>Riggins</u>'s system first downloads the applet 388, and then the downloaded applet 288

authenticates the user and services on a servlet host engine 386,[11] as explained above, <u>Hudson</u>

explains that temporary credential token 52 is created, and subsequently, the user's identifier

authentication information is verified by accessing the resources 56 in an access list.[12]

Accordingly, <u>Hudson</u> fails to teach or suggest that *in response to said authorization* said

administration computer is configured to be linked to a web server that issues said electronic

badge to the visitor's computer, since in <u>Riggins</u> as well as in <u>Hudson</u>, the downloaded applet

288 or the temporary credential token 52 are already present on the host engine 386 or the

access control system 50, respectively.

Regarding the rejection of Applicant's dependent Claim 15 under 35 U.S.C. §103(a),

Applicant traverses the rejection and requests reconsideration of the rejection. While the

outstanding Office Action confirms that the references <u>Riggins</u> and <u>Hudson</u> fail to teach or

suggest the features of dependent Claim 15, the Office Action states that the reference

<u>Montulli</u> teaches such a feature, and that a "cookie is functionally equivalent to the electronic

badge."[13] Applicant respectfully disagrees with these statements. <u>Montulli</u> explains in the

Abstract that a cookie is used to transmit *state information* from a server computer to a client

---

[11] See <u>Riggins</u> for example at column 6, lines 38-50.
[12] See <u>Hudson</u> from column 2, line 64, to column 3, line 7.
[13] See the outstanding Office Action at page 7, lines 17-20.

computer, and <u>Montulli</u> explains, as a person of ordinary skill in the art knows, that cookies represent state information of a URL.[14] Accordingly, state information of a URL, *is not* an electronic badge including access rights conferring access of the visitor's computer. It is also known by a person of ordinary skill in the art that cookies are files that are stored in a single folder, while applets are executable software, that, once executed, cannot be deleted by a simple file deletion, as proposed by <u>Montulli</u>.

Therefore, even if *in arguendo* the combination of <u>Riggins</u>, <u>Hudson</u> and <u>Montulli</u> is proper, the combination fails to teach or suggest all the features of Applicant's dependent claims, and therefore requests reconsideration of these rejections.

For the same reason, Applicant believes that it is improper to combine <u>Riggins</u> with <u>Montulli</u>, since such combination would require a substantial redesign of <u>Riggins</u>' applet technology. There is no evidence that a person of ordinary skill in the art would be motivated to perform such changes and redesign.[15]

Regarding the remaining references <u>Scheifler</u>, <u>Daly</u> and <u>Susaki</u>, these references also fail to remedy the deficiencies of <u>Riggins</u>, <u>Hudson</u> and <u>Montulli</u>. Accordingly, even if we assume that the combination of any of these references is proper, the combination fails to teach or suggest the electronic badge, as recited in Applicant's independent claims. Therefore, Applicant also traverses the other outstanding 35 U.S.C. § 103(a) rejections, and requests reconsideration thereof.

Consequently, in view of the present amendment, no further issues are believed to be outstanding in the present application, and the present application is believed to be in

---

[14] See <u>Montulli</u> at column 7, lines 11-27.
[15] See <u>In re Ratti</u>, 270 F.2d 810, 813, 123 USPQ 349, 352 (reversing an obviousness rejection where the "suggested combination of references would require a substantial reconstruction and redesign of the elements shown in [the primary reference] as well as a change in the basic principle under which the [primary reference] construction was designed to operate.")

condition for formal Allowance. A Notice of Allowance for Claims 1-10, 12-26, 28-41, 43, and 44-47 is earnestly solicited.

Should the Examiner deem that any further action is necessary to place this application in even better form for allowance, the Examiner is encouraged to contact Applicant's undersigned representative at the below listed telephone number.

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.

Gregory J. Maier
Attorney of Record
Registration No. 25,599

Raymond F. Cardillo
Registration No. 40,440

Surinder Sachar
Registration No. 34,423

Customer Number

22850

Tel: (703) 413-3000
Fax: (703) 413 -2220
(OSMMN 06/04)

I:\ATTY\NS\002867\197593US\197593US-AM-DRAFT.DOC

18